Idempotent Generators of Generalized and Double Generalized Quadratic Residue Codes

Bojilov, A.; Dodunekov, S.M.; van Zanten, A.J.

Publication date:
2011

Tilburg center for Creative Computing
Tilburg University
http://www.uvt.nl/ticc

P.O. Box 90153
5000 LE Tilburg, The Netherlands
Email: ticc@uvt.nl

December 22, 2011

TiCC TR 2011-003

Idempotent Generatos of Generalized and Double Generalized Quadratic Residue Codes

TiCC, Tilburg University

and

Bulgarian Academy of Sciences, Bulgaria

A.J. van Zanten, A. Bojilov
and
S.M. Dodunekov

Idempotent Generators of Generalized and Double Generalized Quadratic Residue Codes

TiCC, Tilburg University
and
Bulgarian Academy of Sciences

A.J. van Zanten, A. Bojilov
and
S.M. Dodunekov

Abstract

In this report we continue our work on the idempotent generators of generalized residue codes (*GR*-codes). Explicit expressions for these generators are derived for the quadratic residue codes (*QR*-codes), generalized quadratic residue codes (*GQR*-codes), double generalized quadratic residue codes (*DGQR*-codes) and for the codes of type $C^i_{2^\lambda,q,2}$. All these codes belong to the subclass of *GR*-codes $C^i_{n,q,t}$ with $t=2$.

Contents

1. Introduction p. 4

2. Preliminaries p.5

3. Idempotent generators for *QR*-codes p. 7

4. Idempotent generators for *GQR*-codes p. 14

5. Idempotent generators for *GR*-codes of type $C^{i}_{2^{\lambda},q,2}$ p. 21

6. Idempotent generators for *DGQR*-codes p. 26

References p. 37

1. Introduction

In [3] we introduced the notion of generalized residue codes (*GR*-codes) $C^i_{n,q,t}$, $1 \le i \le t$, of length *n* over $GF(q)$, with *q* some prime power with $(n,q)=1$, where *t* is the index of some subgroup *K* of U_n, such that $K \supseteq H := < q >$, and where U_n is the subgroup consisting of all elements of $\{i \mid (i,n)=1, 1 \le i < n\}$ which are multiplied among each other mod n. These codes are cyclic. For fixed values of *n, q* and *t,* they are equivalent and generated by polynomials $g^{(i)}(x) = \prod_{l \in K_i} (x - \zeta^l)$, $1 \le i \le t$, where ζ is a primitive n^{th} root of unity, while K_i is one of the cosets of K with respect to U_n. In particular, one can take $K = H$, as will be done frequently in this report. In that case the polynomials $g^{(i)}(x)$ can be identified with the $t = \varphi(n)/r$ irreducible polynomials $P_i(x)$, $1 \le i \le t$, of degree *r*, $r =$ ord$_n(q)$, contained in $\Phi_n(x)$, the n^{th} cyclotomic polynomial in $GF(q)[x]$. In the general case $K \supseteq H$, the generators $g^{(i)}(x)$ are products of these irreducible polynomials. For a more extended discussion and for general properties of these codes, we refer to [3].

Among other properties, it is proved in [3] that if U_n is cyclic, its subgroup *K* of index *t* consists of the *t*-powers (*t*-residues) mod *n.* It is a well-known property that says that U_n is cyclic if and only if $n \in \{2, 4, p^\lambda, p^{2\lambda}\}$, where λ is an arbitrary integer ≥ 1. So, for

these values of *n,* the subgroup *K* is identical to $U_n^{\,t}$, the subgroup of U_n consisting of all *t*-residues, i.e. $U_n^{\,t} := \{a^t \mid a \in U_n\}$.
In [4] we defined a matrix M with $|S|$ rows and $|S|$ columns, where S stands for the index set of the cyclotomic cosets mod *n* with respect to *q.* A column with label $i \in S$ determines the primitive idempotent generator $\theta_i(x)$ which corresponds to the cyclotomic coset C_i which on its turn corresponds to the irreducible polynomial $P_i(x) \in GF(q)[x]$. In this sense, the columns of *M* determine the primitive idempotent generators of the minimal cyclic codes of length *n* over $GF(q)$ generated by $\hat{P_i}(x) := x^n - 1/P_i(x)$. Here, the adjective minimal refers to the fact that the ideal $<\hat{P_i}(x)>$ has no subideals except the zero-ideal. As a consequence, by taking sums of primitive idempotent generators in $GF(q)[x]$, the idempotent generators of all cyclic codes of length *n* over $GF(q)$ can be determined. In [4] the labeling of the matrix *M* was chosen such, that the first row and column correspond to $P_0(x) = x - 1$, or equivalently to $C_0 = \{0\}$, and the next *t* rows and columns to the *t* irreducible polynomials $P_i(x)$, contained in $\Phi_n(x)$. The actual values of the indices are the elements of $S \cap U_n$. It also follows easily (cf. again [3]) that $1 - \theta_i(x)$ is the idempotent generator of the cyclic code generated by $P_i(x)$, i.e..the *GR*-code $C^i_{n,q,t}$, $i \in S \cap U_n$. Therefore, we now index the *GR*-codes (for fixed *n, q* and *t*) by the elements of $S \cap U_n$ instead of 1, 2,…,*t*. The remaining rows and columns of M correspond to irreducible polynomials contained in cyclotomic polynomials $\Phi_k(x)$, $k \mid n$ and $1 \le k < n$.
It is shown in [4] that the matrix M has a number of orthogonality and symmetry properties. These properties can be helpful to determine the columns of *M* which stand for the idempotent generators of *GR*-codes. In this report we shall determine the idempotent generators of the codes $C^i_{p^\lambda,q,2}$, $i \in \{1,2\}$, $\lambda \ge 1$, *p* prime, known as (*generalized*) *quadratic residue codes* ((G)QR-*codes*)(cf. [7,8,9,10]), and also for the codes $C^i_{2p^\lambda,q,2}$, $i \in \{1,2\}$, $\lambda \ge 1$, *p* an odd prime, which we shall call *double generalized quadratic residue codes* (*DGQR-codes*). The idempotent generators of *GQR*-codes were already known, and can be found e.g. in [8,9,10] (*QR*-codes) and in [7] (*GQR*-codes). As for the idempotent generators of *DGQR*-codes, it came recently to our attention that expressions for these idempotents are derived in [1] and [2], by quite a different method.

2. Preliminaries

In Section 3 we shall derive explicit expressions for the idempotent generators of codes of length p^λ, with p an odd prime, over $GF(q)$, q some prime power, and for $t = 2$, i.e. for so-called generalized quadratic residue codes (*GQR*-codes). As preparation we first present a few lemmas which will be helpful to distinguish between the cases when

-1 is a quadratic residue mod p^λ and when it is not. The first lemma is Proposition 4.2.3 in [5].

Lemma 1

Let p be an odd prime which does not divide a and m. Then if $x^m = a \mod p$ *is solvable, so is* $x^m = a \mod p^e$ *for all* $e \geq 1$. *All these congruences have the same number of solutions.*

By taking $m = 2$, $a = -1$, $e = \lambda$ and applying the well-known result that -1 is a quadratic residue mod p if and only if $p = 1$ mod 4, we obtain part (i) of the next lemma. Part (ii) is obtained by taking $m = 2$, $a = 2$, $e = \lambda$ and applying the property that 2 is a quadratic residue if and only if $p = \pm 1$ mod 8.

Lemma 2

Let p be an odd prime and let λ *be some integer* ≥ 1. *Then the following holds.*

(i) -1 *is a quadratic residue mod* p^λ *if and only if* $p = 1$ *mod 4*;

(ii) 2 *is a quadratic residue mod* p^λ *if and only if* $p = \pm 1$ *mod 8.*

We also present for a possible future application a property relating the solutions of $x^2 = -1 \mod p$ to the solutions of $x^2 = -1 \mod p^\lambda$ for different values of λ.

Lemma 3

Let p be an odd prime and let p=1 mod 4. Let λ *be an integer* ≥ 1. *If b is a solution of* $x^2 = -1$ *mod p, then* b^p *is a solution of* $x^2 = -1$ *mod* p^λ.

Proof

We shall prove this result by mathematical induction on λ.

For $\lambda = 1$ the Lemma is well-known (cf. e.g. [5]).

Assume that for $p = 1 \mod 4$ we have that -1 is a square mod p^λ for a certain fixed $\lambda \geq 1$. Then we can write

$$-1 = b^2 + k_\lambda p^\lambda, \quad (b, p) = 1, \quad b, k_\lambda \in \mathbb{Z},$$

or equivalently

$$b^2 = -1 - k_\lambda p^\lambda.$$

It follows that

$$b^{2p} = (-1 - k_\lambda p^\lambda)^p = -\sum_{l=0}^{p} \binom{p}{l} (k_\lambda p^\lambda)^l.$$

$$= -1 - k_\lambda p^{\lambda+1} - \sum_{l=2}^{p-1} \binom{p}{l} (k_\lambda p^\lambda)^l - k_\lambda p^{p\lambda}.$$

Since $p \mid \binom{p}{l}$ for all $l \in \{2,3,....,p-1\}$, all terms in the summand are divisible by $p^{\lambda+2}$. Moreover, since p is odd, we have $p\lambda \geq 3\lambda \geq \lambda + 2$, and so the last term is also divisible by $p^{\lambda+2}$. Hence, we can write

$$(b^p)^2 = -1 - k_{\lambda+1} p^{\lambda+1},$$

with $(b^p, p) = 1$, $b^p, k_{\lambda+1} \in \mathbb{Z}$. Therefore, -1 is a square mod $p^{\lambda+1}$. By the principle of mathematical induction we may conclude that -1 is a square mod p^{λ} for all $\lambda \geq 1$. □

For further applications to codes of length $2p^{\lambda}$ in Section 4, we also present a condition for the existence of solutions of the equation $x^2 = a \mod n$ when n is an arbitrary integer. According to Proposition 5.1.1 in [5] we have the following criterion.

Lemma 4

Let $n = 2^e p_1^{e_1} .....p_l^{e_l}$ be the prime decomposition of n, and suppose that $(a,n) = 1$. Then $x^2 = a \mod n$ is solvable if and only if the following conditions are satisfied:

(i) *if $e = 2$, then $a = 1 \mod 4$*;

(ii) *if $e \geq 3$, then $a = 1 \mod 8$*;

(iii) *for each i one has $a^{(p_i-1)/2} = 1 \mod p_i$.*

3. Idempotent generators for *QR*-codes

For the definition of generalized quadratic residue codes (*GQR*-codes) we refer to [3]. Here, we only remind the reader that *GQR*-codes are generalized residue codes of length $n = p^{\lambda}$ over $GF(q)$ for some odd prime *p* and some prime power q, $(p,q) = 1$, and such that the parameter t has value 2. In that case $C^i_{n,q,2}$, $i \in \{1,2\}$, are both 2-residue codes, meaning that the group $K \subseteq U_n$ consists of all quadratic residues mod n (cf. [3]). The group U_n is cyclic for $n = p^{\lambda}$ and so is K. The choice $t = 2$ implies that *q* has to be a quadratic residue itself. We choose *q* such that it generates *K* which itself has index 2 with respect to U_n. Consequently, $H := < q > = K$, and $s = 1$, $\kappa = st = 2$ and $r := \mathrm{ord}_n(q) = \varphi(n)/2$. In the next we shall denote the group of quadratic residues mod *n* by Q_n, or just by Q when it is clear from the context what value *n* has. Hence, under the above condititions the group *K* is identical to Q_n.

For reasons of convenience, we first consider the case $\lambda = 1$, i.e. the subfamily of the conventional quadratic residue codes (*QR*-codes). In this case $\varphi(n) = \varphi(p) = p - 1$, so

$$r = (p-1)/2 . \tag{1}$$

The two nonzero cyclic cosets mod p with respect to q are $C_1 = \{1, q, ..., q^{r-1}\}$ and $C_a = \{a, aq, ..., aq^{r-1}\}$, where a is some non-quadratic residue or nonsquare mod p. If $p = -1 \bmod 4$, we can take $a = -1$, and if $p = 1 \bmod 4$, $a \neq -1$, since -1 is a square in that case. Because there are three cyclotomic cosets, the matrix M is a $3 \times 3-$matrix, which is of the form

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & a \end{matrix} \\ \begin{pmatrix} 1 & r & r \\ 1 & \alpha & \beta \\ 1 & \beta & \alpha \end{pmatrix} \begin{matrix} 0 \\ 1 \\ a \end{matrix} \end{array}, \qquad \alpha, \beta \in GF(q). \tag{2}$$

Remember that the third column has to be a permutation of the second one (cf. [4]). The only possible permutation unequal to the identity is obtained by interchanging the second and third entry.

.

(i) $p = 1 \bmod 4$

In this case -1 is a quadratic residue mod p, and so $-1 \in C_1$ and $a \neq -1$.First we consider the case q is odd. The orthogonality relations of [4, Theorem 28 (i)] provide us with

$$1 + \alpha + \beta = 0, \tag{3}$$

$$r + \alpha^2 + \beta^2 = p, \tag{4}$$

$$r + 2\alpha\beta = 0. \tag{5}$$

Substituting (3) in (4) and (5) gives

$$2r + 1 = p, \tag{6}$$

$$(2\alpha + 1)^2 = p, \tag{7}$$

resulting in

$$\alpha = \frac{-1 + \sqrt{p}}{2}, \quad \beta = \frac{-1 - \sqrt{p}}{2}. \tag{8}$$

Hence, the primitive idempotent generators of the cyclic codes generated by columns 1 and a are

$$\theta_1(x) = p^{-1}(r + \alpha \sum_{i \in C_1} x^i + \beta \sum_{i \in C_a} x^i) \tag{9}$$

and

$$\theta_2(x) = p^{-1}(r + \beta \sum_{i \in C_1} x^i + \alpha \sum_{i \in C_a} x^i), \tag{10}$$

with α and β as defined in (8). All coefficients have to be interpreted as elements of $GF(q)$. The idempotent generators of the *QR*-codes $C^i_{p,q,2}$, are $\vartheta_i(x) = 1 - \theta_i(x)$, $i \in \{1, a\}$.

Since we know that the above idempotent generators are uniquely determined, we are entitled to conclude that p is a quadratic residue mod q, and consequently there exist precisely two solutions of the equation $x^2 = p$ in $GF(q)$ under the assumptions made in this case. If we choose one of these to be $\sqrt{p}$, the other is $-\sqrt{p}$. The remaining question is how to choose $\sqrt{p}$ in order that $\theta_1(x)$ corresponds to the column of M with index 1, and $\theta_a(x)$ with the column indexed by *a*. More precisely, the remaining question is to which of the two irreducible factors of $\Phi_p(x)$ the idempotent generator $\theta_1(x)$ corresponds. Notice that we computed $\theta_1(x)$ and $\theta_a(x)$ without using or even defining the primitive p^{th} root ζ, i.e. without selecting the defining polynomial of ζ.

Next, we consider the case q even, i.e. $q = 2^m$. The equations (3) and (4) now take the form

$$1 + \alpha + \beta = 0, \tag{11}$$

$$\alpha^2 + \beta^2 = 1. \tag{12}$$

Observe that eq. (5) is trivially satisfied now, because $r = 0$ in the case $p = 1 \bmod 4$ (cf. eq. (1)). Furthermore, if α and β are chosen such that eq. (11) holds, eq. (12) follows immediately by squaring both sides of (11). It follows that by putting $\alpha := \xi$ for some arbitrary element ξ of $GF(2^m)$ and by taking $\beta = 1 + \xi$, we obtain a solution. However, only solutions $(\alpha, \beta) \in \{(1,0),(0,1),(\xi,\xi^2),(\xi^2,\xi)\}$ with $\xi^2 + \xi + 1 = 0$ are allowed. We can see this as follows. If $p = 1 \bmod 8$ then $2 \in Q$ (cf. Lemma 2) and hence, since 2^m is assumed to generate Q, 2 also generates Q and $\mathrm{ord}_p(2) = \mathrm{ord}_p(2^m) = (p-1)/2$. So, the splitting of $\Phi_p(x)$ into two irreducible polynomials over $GF(2^m)$ is the same as over $GF(2)$ and the elements of the matrix M are actually in $GF(2)$. So, $\alpha = 1$, $\beta = 0$ or $\alpha = 0$, $\beta = 1$.

If $p = -3 \mod 8$, then $2 \notin Q$. Since we required that $q = 2^m$ generates $K(=Q)$, we now have again $\text{ord}_p(q^m) = (p-1)/2$, but $\text{ord}_p(q) = p-1$. Hence, 2^2 generates Q and m must be even. So, the splitting of $\Phi_p(x)$ into two irreducible polynomials over $GF(2^m)$ is the same as over $GF(2^2)$. Hence, $\alpha = \xi$, $\beta = \xi^2$ or $\alpha = \xi^2$, $\beta = \xi$ in that case.

(ii) $p = -1 \mod 4$

In this case -1 is not a quadratic residue and so $-1 \in C_a$ and we can put $a = -1$.
First, let q be odd. The relations [4, Theorem 28 (i)] now give

$$1 + \alpha + \beta = 0 \tag{13}$$

$$r + 2\alpha\beta = p\,, \tag{14}$$

$$r + \alpha^2 + \beta^2 = 0\,. \tag{15}$$

Adding and subtracting (14) and (15) and substituting (13) gives

$$2r + 1 = p\,, \tag{16}$$

$$(2\alpha + 1)^2 = -p\,, \tag{17}$$

providing us with the solution

$$\alpha = \frac{-1 + \sqrt{-p}}{2}, \quad \beta = \frac{-1 - \sqrt{-p}}{2}\,. \tag{18}$$

So, the primitive idempotent generators corresponding to the second and third column are

$$\theta_1(x) = p^{-1}(r + \alpha \sum_{i \in C_1} x^i + \beta \sum_{i \in C_a} x^i)\,, \tag{19}$$

and

$$\theta_{-1}(x) = p^{-1}(r + \alpha \sum_{i \in C_1} x^i + \beta \sum_{i \in C_{-1}} x^i)\,, \tag{20}$$

with α and β as defined in (18).
Similar remarks as in the case $p = 1 \mod 4$ can be made with respect to these expressions and their relationship with the irreducible factors of $\Phi_p(x)$.

Finally, we take $q = 2^m$. The equations (13) and (15) take the form

$$1+\alpha+\beta=0\,, \tag{21}$$

$$1+\alpha^2+\beta^2=0\,. \tag{22}$$

Equation (14) is again trivially satisfied, since $r=1$ in the case $p=-1 \bmod 4$.
Similarly as in the case $p=1 \bmod 4$, we now find that $\alpha=1$, $\beta=0$ or $\alpha=0$, $\beta=1$, if $p=-1 \bmod 8$ and $\alpha=\xi$, $\beta=\xi^2$ or $\alpha=\xi^2$, $\beta=\xi$, if $p=3 \bmod 8$.

Example 5
Take $p=11$. The group of quadratic residues mod p is $Q_{11}=\{1,4,9,5,3\}$. All its elements $\neq 1$ are generators of Q_{11}, so we can take any of these elements as value of the prime power q. For all these q we have $r=\operatorname{ord}_{11}(q)=5$. Since $11=-1 \bmod 4$, we are in case (ii) and we may use (18) to determine idempotent generators in the case q is odd.

a. If $q=3$ we have $p=2$ in $GF(3)$ and $\sqrt{-11}=1$. So the matrix M equals

$$M=\begin{pmatrix}1 & 2 & 2\\ 1 & 0 & -1\\ 1 & -1 & 0\end{pmatrix}.$$

The matrix elements 0 and -1 correspond to the coefficients of x^4 in
$P_1(x)=x^5-x^3+x^2+x-1$ and $P_2(x)=x^5+x^4-x^3+x^2-1$ (cf. [3,Example 5.3]),
which are the irreducible factors of $\Phi_{11}(x)$ over $GF(3)$.
The primitive idempotent generators are

$$\theta_1(x)=11^{-1}(2c_0(x)-c_{-1}(x))=1+x^2+x^6+x^7+x^8+x^{10}$$

and

$$\theta_{-1}(x)=11^{-1}(2c_0(x)-c_1(x))=1+x+x^3+x^4+x^5+x^9\,.$$

For the idempotent generators of the codes $C^1_{11,3,2}$ and $C^2_{11,3,2}$ we find

$$\vartheta_1^*(x)=\vartheta_{-1}(x)=1-\theta_{-1}(x)=-(x+x^3+x^4+x^5+x^9)$$

and

$$\vartheta_{-1}{}^*(x)=\vartheta_1(x)=1-\theta_1(x)=-(x^2+x^6+x^7+x^8+x^{10})\,.$$

These expressions were also derived in [8, Ch. 16, Section 3].

b. If $q = 5$, we have $p = 1$ in $GF(5)$ and $\sqrt{-11} = \sqrt{4} = 2$, and hence

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & 1 \\ 1 & 1 & 3 \end{pmatrix}.$$

The matrix elements $3(=-2)$ and 1 correspond to the coefficients of x^4 in $P_1(x) = x^5 + 2x^4 - x^3 + x^2 + x - 1$ and $P_2(x) = x^5 - x^4 - x^3 + x^2 - 2x - 1$, which are the irreducible factors of $\Phi_{11}(x)$ over $GF(5)$.
The primitive idempotent generators are

$$\theta_1(x) = 11^{-1}(3c_1(x) + c_{-1}(x)) = 3x + 3x^3 + 3x^5 + 3x^9 - x^2 - x^6 - x^7 - x^8 - x^{10}$$

and

$$\theta_{-1}(x) = 11^{-1}(c_1(x) + 3c_{-1}(x)) = x + x^3 + x^4 + x^5 + x^9 + 3x^2 + 3x^6 + 3x^7 + 3x^8 + 3x^{10}.$$

c. If $q = 4$, we have $p = 1$ in $GF(4)$. Moreover, since $\mathrm{ord}_{11}(2) = 10$, there is no decomposition of $\Phi_{11}(x)$ into two irreducible polynomials in $GF(2)$. Notice that $2 \notin Q$ and that $q = 2^m$ with $m(=2)$ even, and hence 4 generates Q. Consequently the solutions $\alpha = 1$, $\beta = 0$ and $\alpha = 0$, $\beta = 1$ do not apply here. We have to take $\alpha = \xi$, $\beta = \xi^2$ or $\alpha = \xi^2$, $\beta = \xi$, since $p = 3$ mod 8 in this case (cf. the previous page), and hence we have the following matrix over GF(4)

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \xi & \xi^2 \\ 1 & \xi^2 & \xi \end{pmatrix},$$

where ξ is defined by the equation

$$\xi^2 + \xi + 1 = 0.$$

The second and third column of the matrix M which determine the primitive idempotent generators of $C^i_{11,4,2}$, $i \in \{1,2\}$, are in line with the irreducible polynomials $P_1(x)$ and $P_2(x)$ over $GF(4)$ in the decomposition

$$\Phi_{11}(x) = P_1(x)P_2(x) = (x^5 + \xi x^4 + x^3 + x^2 + \xi^2 x + 1)(x^5 + \xi^2 x^4 + x^3 + x^2 + \xi x + 1),$$

yielding $p_{1,1} = \xi$ and $p_{2,1} = \xi^2$ (cf. [3, Example 5.3]).

The primitive idempotent generators are

$$\begin{aligned}\theta_1(x) &= 11^{-1}(c_0(x) + \xi c_1(x) + \xi^2 c_{-1}(x)) \\ &= 1 + \xi(x + x^3 + x^4 + x^5 + x^9) + \xi^2(x^2 + x^6 + x^7 + x^8 + x^{10})\end{aligned}$$

and

$$\begin{aligned}\theta_2(x) &= 11^{-1}(c_0(x) + \xi^2 c_1(x) + \xi c_{-1}(x)) \\ &= 1 + \xi^2(x + x^3 + x^4 + x^5 + x^9) + \xi(x^2 + x^6 + x^7 + x^8 + x^{10}).\end{aligned}$$

d. If $q = 9$, then $p = 2$ in $GF(9)$. Since $\text{ord}_{11}(9) = 5$ and hence $\kappa = 10/5 = 2$, we have again that $\Phi_{11}(x)$ is the product of two irreducible polynomials, this time over the field $GF(9)$. We conclude that the polynomials $P_1(x)$ and $P_2(x)$ in case a do not split when extending $GF(3)$ to $GF(9)$. Applying (18) with $\sqrt{-11} = \sqrt{1} = 1$, we find that $\alpha = 0$, $\beta = -1$ and $\alpha = -1$, $\beta = 0$ satisfy all conditions now interpreted as equations in $GF(9)$. So, we have the following matrix M in this case

$$M = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix},$$

which gives rise to the idempotent generators

$$\theta_1(x) = 11^{-1}(2c_0(x) - c_{-1}(x)) = 1 + x^2 + x^6 + x^7 + x^8 + x^{10}$$

and

$$\theta_{-1}(x) = 11^{-1}(2c_0(x) - c_1(x)) = 1 + x + x^3 + x^4 + x^5 + x^9.$$

In all cases a – d we verified the idempotency relation $\theta_i(x)^2 = \theta_i(x)$. □

Of course, one also can compute the elements of the matrix *M*, and hence the idempotent generators, straightforwardly. Let us do so in the case of $p = 1 \bmod 4$.
We have from [4, eq. 27] that

$$\mu_{1,1} = -p_{1,1}, \qquad \mu_{2,1} = -p_{2,1}. \tag{23}$$

Since

$$P_1(x) = \sum_{i \in K_1}(x - \zeta^i) = \sum_{i \in C_1}(x - \zeta^i), \tag{24}$$

it follows that

$$p_{1,1} = -\sum_{i \in C_1} \zeta^i \,. \tag{25}$$

Analogously, we find

$$p_{2,1} = -\sum_{i \in C_a} \zeta^i \,. \tag{26}$$

Now, the sum and the difference of the rhs of eqs. (19) and (20) are equal to respectively

$$\sum_{i \in C_1} \zeta^i + \sum_{i \in C_a} \zeta^i = \sum_{i=1}^{q-1} \zeta^i = -1\,, \tag{27}$$

$$\sum_{i \in C_1} \zeta^i - \sum_{i \in C_a} \zeta^i = G_q(2)\,. \tag{28}$$

The notation $G_q(2)$ stands for the Gauss sum $G(2)$ taken as an element in $GF(q)$.
So, by putting $\alpha = \mu_{1,1}$ and $\beta = \mu_{2,1}$ and using (25) and (26), we find

$$\alpha = \frac{-1 + G_q(2)}{2}\,, \quad \beta = \frac{-1 + G_q(2)}{2}\,. \tag{29}$$

From the literature (cf. [6]) it is known that for $p = 1 \bmod 4$, the value of $G(2)$ is equal to $+\sqrt{p}$. Substituting $G_q(2) = \sqrt{p}$ in (29) gives the expressions for $\theta_1^*(x)$ and $\theta_a^*(x)$ as presented in (9) and (10).
We conclude that the problem of how to define $\sqrt{p}$ in $GF(q)$ such that the idempotent generators of (19) and (20) correspond to the right cyclotomic coset or to the right column of *M*, is the *q*-analogon of the famous problem of how to determine the sign of the Gauss sum $G(2)$, after having determined its absolute value $\sqrt{p}$.
In case (ii), when $p = -1 \bmod 4$, similar considerations apply. For this *p*-value one has $G(2) = i\sqrt{p}$.

4. Idempotent generators for *GQR*-codes

Next, we take $n = p^\lambda$, $\lambda \geq 1$, and again *q* an arbitrary prime power such that $(p,q) = 1$. We also assume again that *q* generates the subgroup *K* $(= Q := Q_{p^\lambda})$ of U_n consisting of quadratic residues mod p^λ, which are prime to *n*. Just like in the case $\lambda = 1$, it follows that *K* is a subgroup of U_{p^λ} of index 2. The group U_{p^λ} itself has order

$\varphi(p^\lambda) = p^{\lambda-1}(p-1)$. In [4, eq. (64)]] we labeled the rows and columns of the matrix *M* by the integers

$$0, i_1^\lambda, i_2^\lambda, ..., i_{\kappa_\lambda}^\lambda, i_1^{\lambda-1}, i_2^{\lambda-1}, ..., i_{\kappa_{\lambda-1}}^{\lambda-1}, ..., i_1^1, i_2^1, ..., i_{\kappa_1}^1, \tag{30}$$

with $i_1^\lambda = 1$. These integers represent the cyclotomic cosets mod p^λ to which they belong. The subindices κ_b, $1 \le b \le \lambda$, can be obtained from $\kappa_b = \varphi(p^b)/r_b$, where $r_b := \text{ord}_{p^b}(q)$ is equal to the degree of the irreducible polynomials contained in $\Phi_{p^b}(x)$ or to the size of the corresponding cyclotomic cosets mod p^b. Together the indices (30) constitute the index set *S*. However, the value of the index of a particular cyclotomic coset is not uniquely determined. One convention (cf. [3]) is to take the least integer of that cyclotomic coset, but this cannot be maintained in a consistent way when calculations with the indices have to be carried out like in our theory of the matrix *M*. Especially, when one takes into account the mutual relationship between the cosets with respect to multiplication by some integer *a*, expressed by $iC_a = C_{ia}$. The order of the indices in (30) is chosen such that the column indices $i_1^b, i_2^b, ..., i_{\kappa_b}^b$, $1 \le b \le \lambda$, indicate the κ_b irreducible polynomials $P_{i_j^b}(x)$ of degree r_b which are contained in $\Phi_{p^b}(x)$, whereas when interpreted as row indices, they stand for the corresponding cyclonomials $c_i(x)$. Our case was defined by the requirement $\kappa_\lambda = t = 2$. In [4, Lemma 58] we proved that for $n = p^\lambda$ and $\kappa_\lambda = 2$, one has to distinguish between the following cases

$$2 = \kappa_1 = \kappa_2 = ..., \text{ for } p \text{ odd}, \tag{31}$$

$$1 = \kappa_1 < 2 = \kappa_2 = \kappa_3 = ..., \text{ for } p = 2,\ q = 1 + 4l,\ l \text{ odd}, \tag{32}$$

$$1 = \kappa_1 < 2 = \kappa_2 < 4 = \kappa_3 \le \kappa_4 \le .... \text{ , for } p = 2,\ q = 1 + 4l,\ l \text{ even}, \tag{33}$$

$$1 = \kappa_1 = \kappa_2 < 2 = \kappa_3 = \kappa_4 = ..., \text{ for } p = 2,\ q = -1 + 4l,\ l \text{ odd}, \tag{34}$$

$$1 = \kappa_1 = \kappa_2 < 2 = \kappa_3 < 4 = \kappa_4 \le \kappa_5 \le ...., \text{ for } p = 2,\ q = -1 + 4l,\ l \text{ even}. \tag{35}$$

We conclude that in these cases one has $\lambda \ge 1$, $\lambda \ge 2$, $\lambda = 2$, $\lambda \ge 3$ and $\lambda = 3$, respectively.

Since *QR*-codes were primarily defined for odd values of the prime *p*, we start with the case (31). This implies that *M* is a $(2\lambda+1)\times(2\lambda+1)$-matrix. We showed in [4] (cf. [4, eq. (57)]) that the general form of *M* in this case is equal to

$$M = \begin{array}{c} \begin{array}{cccccccccc} 0 & i_1^{\lambda} & i_2^{\lambda} & i_1^{\lambda-1} & i_2^{\lambda-1} & . & . & i_1^1 & i_2^1 & \end{array} \\ \begin{pmatrix} 1 & r_\lambda & r_\lambda & r_{\lambda-1} & r_{\lambda-1} & . & . & r_1 & r_1 & 0 \\ 1 & 0 & 0 & . & . & . & . & p^{1-\lambda}\alpha & p^{1-\lambda}\beta & i_1^{\lambda} \\ 1 & 0 & 0 & . & . & . & . & p^{1-\lambda}\beta & p^{1-\lambda}\alpha & i_2^{\lambda} \\ . & . & . & . & . & . & . & . & . & i_1^{\lambda-1} \\ . & . & . & . & . & . & . & . & . & i_2^{\lambda-1} \\ 1 & 0 & 0 & . & . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & . & . & . & . & . \\ 1 & \alpha & \beta & . & . & . & . & . & . & i_1^1 \\ 1 & \beta & \alpha & . & . & . & . & . & . & i_2^1 \end{pmatrix} \end{array} . \tag{36}$$

For the integers $r_b := \mathrm{ord}_{p^b}(q)$, which represent the size of the cyclotomic cosets mod p^b, we have in general (cf. [4, Lemma 57 (i) with $d = 1$])

$$r_b = r_1 p^{b-1}, \quad 1 \le b \le \lambda. \tag{37}$$

Furthermore, due to our choice of q being a generator of the group of quadratic residues mod p^{λ},

$$r_\lambda = \varphi(p^\lambda)/2, \tag{38}$$

and hence

$$r_b = p^{b-\lambda}\varphi(p^\lambda)/2 = p^{b-1}(p-1)/2, \ 1 \le b \le \lambda. \tag{39}$$

The columns with index $i_1^{\lambda}(=1)$ and i_2^{λ} determine the primitive idempotent generators $\theta_{i_1^{\lambda}}(x)(=\theta_1(x))$ and $\theta_{i_2^{\lambda}}(x)(=\theta_a(x))$. By means of the relation $\vartheta_i^*(x) = \vartheta_{-i}(x) = 1 - \theta_{-i}(x)$, $i \in \{i_1^{\lambda}, i_2^{\lambda}\}$, the idempotent generators of the *GQR*- codes then follow.

Assume $p = 1 \bmod 4$. Hence, -1 is a square mod p^{λ} (cf. Lemma 2(i)), and so $a \neq -1$. First we consider the case that q is odd. Applying the relations of [4, Theorem 28] to the first three columns and rows, i.e. to the columns and rows with labels 0, i_1^{λ}, i_2^{λ}, provides us with the equalities

$$r_\lambda + r_1\alpha + r_1\beta = 0 \tag{40}$$

$$r_\lambda + p^{1-\lambda}\alpha^2 + p^{1-\lambda}\beta^2 = p^\lambda, \tag{41}$$

$$r_\lambda + 2p^{1-\lambda}\alpha\beta = 0\,. \tag{42}$$

Applying $r_\lambda = r_1 p^{\lambda-1}$ (cf. eq. (37)) we obtain

$$p^{\lambda-1} + \alpha + \beta = 0\,, \tag{43}$$

$$r_\lambda p^{\lambda-1} + \alpha^2 + \beta^2 = p^{2\lambda-1}\,, \tag{44}$$

$$r_\lambda p^{\lambda-1} + 2\alpha\beta = 0\,. \tag{45}$$

From these relations we obtain in a similar way as for $\lambda = 1$ that

$$\alpha = \frac{-1+\sqrt{p}}{2}\,p^{\lambda-1}\,, \quad \beta = \frac{-1-\sqrt{p}}{2}\,p^{\lambda-1}\,. \tag{46}$$

The primitive idempotent generators corresponding to the columns with index i_1^λ and i_2^λ are

$$\theta_{i_1^\lambda}(x) = p^{-\lambda}(r_\lambda + \alpha c_{i_1^1}(x) + \beta c_{i_2^1}(x)) \tag{47}$$

and

$$\theta_{i_2^\lambda}(x) = p^{-\lambda}(r_\lambda + \beta c_{i_1^1}(x) + \alpha c_{i_2^1}(x))\,. \tag{48}$$

with α and β from (46).

If $p = -1 \mod 4$, then -1 is not a square mod p^λ (cf. Lemma 2(i)), and so $a = -1$ We can argue similarly as in the case $\lambda = 1$. Applying the orthogonality relations of [4, Theorem 28] again, now gives rise to

$$p^{\lambda-1} + \alpha + \beta = 0\,, \tag{49}$$

$$r_\lambda p^{\lambda-1} + \alpha^2 + \beta^2 = 0\,, \tag{50}$$

$$r_\lambda p^{\lambda-1} + 2\alpha\beta = p^{2\lambda-1}\,. \tag{51}$$

We find for the primitive idempotent generators corresponding to columns i_1^λ and i_2^λ the same expressions as (47) and (48), but this time with

$$\alpha = \frac{-1+\sqrt{-p}}{2}\,p^{\lambda-1}\,, \quad \beta = \frac{-1-\sqrt{-p}}{2}\,p^{\lambda-1}\,. \tag{52}$$

As for the existence of the square roots $\sqrt{p}$ and $\sqrt{-p}$ we can make the same remarks as for $\lambda = 1$. We collect all the obtained results in the following theorem. Instead of the

general notation i_1^λ, i_2^λ for the second and third column of the matrix M, we shall use $1(=i_1^\lambda)$ and $a(=i_2^\lambda)$, since we assume that the corresponding cyclotomic cosets are $C_{i_1^\lambda}=C_1=\{1,q,.....,q^{r_\lambda-1}\}$ and $C_{i_2^\lambda}=C_a=\{a,aq,.....,aq^{r_\lambda-1}\}$ for some *a*. The other cyclotomic cosets should consequently be denoted by $C_{p^{\lambda-b}}$ and $C_{ap^{\lambda-b}}$ for $1\le b<\lambda$.

Theorem 6

Let p be some odd prime and q some prime power with $(p,q)=1$ *and let q be a generator of the group* Q_{p^λ} *of quadratic residues mod* p^λ. *Let furthermore, M be the matrix for codes of length* $p^\lambda, \lambda\ge 1$, *over* $GF(q)$, *and with* $t=2$.

(i) *If q is odd, then the two primitive idempotent generators corresponding to the columns indexed by* 1 *and a of the matrix M, can for* $p=1$ *mod 4 be written as*

$$\theta_1(x)=\frac{1}{2p}[p-1+\left(-1+\sqrt{p}\right)\sum_{i\in Q_p}x^{ip^{\lambda-1}}+\left(-1-\sqrt{p}\right)\sum_{i\in Q_p}x^{aip^{\lambda-1}}],$$

$$\theta_a(x)=\frac{1}{2p}[p-1+\left(-1-\sqrt{p}\right)\sum_{i\in Q_p}x^{ip^{\lambda-1}}+\left(-1+\sqrt{p}\right)\sum_{i\in Q_p}x^{ai^{\lambda-1}}],$$

and for $p=-1$ *mod 4 as*

$$\theta_1(x)=\frac{1}{2p}[p-1+\left(-1+\sqrt{-p}\right)\sum_{i\in Q_p}x^{ip^{\lambda-1}}+\left(-1-\sqrt{-p}\right)\sum_{i\in Q_p}x^{-ip^{\lambda-1}}],$$

$$\theta_{-1}(x)=\frac{1}{2p}[p-1+\left(-1-\sqrt{-p}\right)\sum_{i\in Q_p}x^{ip^{\lambda-1}}+\left(-1+\sqrt{-p}\right)\sum_{i\in Q_p}x^{-ip^{\lambda-1}}],$$

where all coefficients are to be taken in $GF(q)$, *and where* $\sqrt{p}$ *and* $\sqrt{-p}$ *have to be selected appropriately from the two possible values in* $GF(q)$.

(ii) *If* $q=2^m$, *then these two primitive idempotent generators can for* $p=\pm1$ *mod 8 be written as*

$$\theta_1(x)=1+\sum_{i\in Q_p}x^{ip^{\lambda-1}},$$

$$\theta_a(x)=1+\sum_{i\notin Q_p}x^{ip^{\lambda-1}},$$

with $a=-1$ *if* $p=-1$ *mod 8 and* $a\ne-1$ *if* $p=1$ *mod 8, while for* $p=\pm3$ *mod 8*

$$\theta_1(x)=1+\xi\sum_{i\in Q_p}x^{ip^{\lambda-1}}+\xi^2\sum_{i\notin Q_p}x^{ip^{\lambda-1}},$$

$$\theta_a(x)=1+\xi^2\sum_{i\in Q_p}x^{ip^{\lambda-1}}+\xi\sum_{i\notin Q_p}x^{ip^{\lambda-1}},$$

with $a=-1$ *if* $p=3$ *mod 8 and* $a\neq -1$ *if* $p=-3$ *mod 8.*

Proof

(i) The proof is analogous to the proof for $\lambda=1$ on the previous pages. Since U_{p^λ} is cyclic for odd primes *p*, its subgroup $K=Q(=Q_{p^\lambda})$ has index 2, because the even powers of some generator of U_{p^λ} are quadratic residues , while the odd powers are non-quadratic residues.Moreover, *Q* is also cyclic and therefore generators which are prime powers may exist.

Lemma 2 (ii) gives that if $p=1$ mod 4, then $a\neq -1$, and if $p=-1$ mod 4, then $a=-1$. First we consider the case $p=1$ mod 4. From (36) it follows that the only nonzero elements in column i_1^λ of *M* are $\mu_{0,i_1^\lambda}=r_\lambda$, $\mu_{i_1^1,,i_1^\lambda}=\alpha$ and $\mu_{i_2^1,i_1^\lambda}=\beta$. Hence,

$$\theta_1(x)=\frac{1}{p^\lambda}[r_\lambda+\alpha c_{i_1^1}(x)+\beta c_{i_2^1}(x)],$$

with α and β from (46), $r_\lambda=\varphi(p^\lambda)=p^{\lambda-1}(p-1)$, $c_{i_1^1}(x)=c_{p^{\lambda-1}}(x)=\sum_{i\in Q_p}x^{ip^{\lambda-1}}$ and $c_{i_2^1}(x)=c_{ap^{\lambda-1}}(x)=\sum_{i\in Q_{p1}}x^{aip^{\lambda-1}}$. Here, we used the relations $C_{p^{\lambda-1}}=p^{\lambda-1}Q_p$ and $C_{ap^{\lambda-1}}=ap^{\lambda-1}Q_p$. The expressions for $\theta_1(x)$ and $\theta_a(x)$ now follow easily. The expressions in case that $p=-1$ mod 4 can be derived similarly.

(ii) Take $q=2^m$. For $p=1$ mod 4 and hence $a\neq -1$, eqs. (43) and (44) take the form $1+\alpha+\beta=0$ and $\alpha^2+\beta^2=1$, respectively, while eq. (45) is trivially satisfied since the value of $r_\lambda=\varphi(p^\lambda)/2=p^{\lambda-1}(p-1)/2$ is even for $p=1$ mod 4. Just like in the case $\lambda=1$, as discussed on p. 9, we find the solutions $\alpha=1,\beta=0$ or $\alpha=0,\beta=1$ if $p=1$ mod 8 and $\alpha=\xi,\beta=\xi^2$ or $\alpha=\xi^2,\beta=\xi$ if $p=-3$ mod 8, while *m* must be even.
For $p=-1$ mod 4, and hence $a=-1$, eqs. (49) and (50) again take the form $1+\alpha+\beta=0$ and $\alpha^2+\beta^2=1$, respectively, while now eq.(51) is trivially satisfied, since r_λ has an odd value in this case. This proves the remaining part of the Theorem. □

Corollary 7

The idempotent generators of the generalized quadratic residue codes $C^i_{p^\lambda,q,2}$*,q some prime power with* (p,q) = 1, $i\in\{1,a\}$*, are given by* $\vartheta_i(x)=1-\theta_i(x)$*, with the polynomials* $\theta_i(x)$ *as defined Theorem 6.*

Remark 8
Of course one can determine the primitive idempotent generators which occur in Theorem 6 more straightforwardly, i.e. not in terms of the matrix *M*. This was accomplished for *QR*-codes ($\lambda = 1$ and q prime) in e.g. [7, 9, 10] and for *GQR*-codes in [8]. Furthermore, we already indicated that the precise correspondence between the expressions in Theorem 6 and the column indices i_1^{λ} (=1) and $i_2^{\lambda} = (a)$ of *M* (which stand for the two irreducible polynomial factors of $\Phi_{p^{\lambda}}(x)$) is still a remaining problem.

However, we don't have to solve this problem if we are only interested in the codes themselves which are defined by these idempotent generators. This demonstrates the fact that in general one can find the idempotent generators of cyclic codes of length n, without factoring $x^n - 1$ into irreducible polynomials (cf. [10, p.77]).

Example 9
Take $n = p^{\lambda} = 27$, i.e. $p = 3$ and $\lambda = 3$. The group of quadratic residues mod 27 is $Q_{27} = \{1,4,7,10,13,16,19,22,25\}$. It appears that 4, 7, 13, 16 and 25 are generators

a. Let $q = 7$. Since $\text{ord}_9(7) = 3 > \text{ord}_3(7) = 1$ we are entitled to apply Theorem 6. If we define $\sqrt{-3} = 2$ in $GF(7)$, we obtain

$$\theta_1(x) = -2 - \sum_{i \in Q_3} x^{9i} + 3\sum_{i \notin Q_3} x^{9i} = -2 - x^9 + 3x^{18},$$

and

$$\theta_{-1}(x) = -2 + 3\sum_{i \in Q_3} x^{9i} - \sum_{i \notin Q_3} x^{9i} = -2 + 3x^9 - x^{18}.$$

The same expressions were computed in [8, Example] by different means

b. Let $q = 13$. Since $\text{ord}_9(13) = 3 > \text{ord}_3(13) = 1$, we may apply again Theorem 6. When defining $\sqrt{-3} = \sqrt{10} = 6$ in $GF(13)$, we find

$$\theta_1(x) = -4 + 3\sum_{i \in Q_3} x^{9i} + \sum_{i \notin Q_3} x^{9i} = -4 + 3x^9 + x^{18},$$

$$\theta_{-1}(x) = -4 + \sum_{i \in Q_3} x^{9i} + 3\sum_{i \notin Q_3} x^{9i} = -4 + x^9 + 3x^{18}.$$

c. Let $q = 25$. Since $\text{ord}_9(25) = 3 > \text{ord}_3(25) = 1$, we may apply Theorem 5. In this case $\sqrt{-3} = \sqrt{2}$ has no solution in $GF(5)$, but it does have in $GF(25)$. To obtain such a solution explicitly, we extend $GF(5)$ by a zero ξ of the irreducible $GF(5)$-polynomial $x^2 + x + 1$. So, $\xi^2 = -\xi - 1$ and one can easily verify that $2\xi + 1$ and $3\xi - 1$ are square roots of 2. We define $\sqrt{2} = 2\xi + 1$. Completely similarly as in a, we now find

$$\theta_1(x) = 2 + 2\xi x^9 - 2(1+\xi)x^{18},$$

and

$$\theta_2(x) = 2 - 2(1+\xi)x^9 + 2\xi x^{18}.$$

d. Let $q = 4$. Since $\mathrm{ord}_9(4) = 3 > \mathrm{ord}_3(4) = 1$, we may apply Theorem 6 (ii) which provides us with the expressions

$$\theta_1(x) = 1 + \xi x^9 + \xi^2 x^{18},$$

and

$$\theta_2(x) = 1 + \xi^2 x^9 + \xi x^{18}.$$

e. Let $q = 16$. Since $GF(4) \subset GF(16)$, the expressions in c are also primitive idempotent generators in $GF(16)[x]$. □

5. Idempotent Generators for *GR*-codes of type $C^i_{2^\lambda,q,2}$

The next case of *GR*-codes with $t = \kappa_\lambda = 2$ are codes of length 2^λ, which are subdivided into four classes by (32) – (34). Strictly speaking, the resulting *GR*-codes are not quadratic residue codes, since now the group $H =< q >$ is not identical to the group of quadratic residues mod 2^λ. Actually, H contains a subgroup of index 2 consisting of quadratic residues, i.e. the even powers of q. All squares of elements of the coset aH, $a \notin H$, are in H. Such a square cannot be equal to an odd power of q, since then U would have a single generator which is false. Therefore, the complete subgroup of quadratic residues is contained in H and is of index 2 w.r.t. H and of index 4 w.r.t. U. It also follows that H can neither be extended to a group K, such that K is identical to the full group of quadratic residues.

Case A

The first class of such codes is characterized by $n = 2^\lambda$, $\lambda \geq 2$, $q = 1 + 4l$, l odd, (cf. (32)). It follows that M is now a $2\lambda \times 2\lambda$-matrix of the form

$$M = \begin{array}{c} \begin{array}{cccccccccc} 0 & i_1^{\lambda} & i_2^{\lambda} & i_1^{\lambda-1} & i_2^{\lambda-1} & . & . & i_1^2 & i_2^2 & i_1^1 \end{array} \\ \begin{pmatrix} 1 & r_\lambda & r_\lambda & r_{\lambda-1} & r_{\lambda-1} & . & . & r_2 & r_2 & r_1 \\ 1 & 0 & 0 & . & . & . & . & 2^{2-\lambda}\alpha & 2^{2-\lambda}\beta & -1 \\ 1 & 0 & 0 & . & . & . & . & 2^{2-\lambda}\beta & 2^{2-\lambda}\alpha & -1 \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & . & . & . & . & . \\ 1 & \alpha & \beta & . & . & . & . & . & . & 1 \\ 1 & \beta & \alpha & . & . & . & . & . & . & 1 \\ 1 & -r_\lambda & -r_\lambda & . & . & . & . & . & . & 1 \end{pmatrix} \end{array} \begin{array}{c} 0 \\ i_1^{\lambda} \\ i_2^{\lambda} \\ i_1^{\lambda-1} \\ i_2^{\lambda-1} \\ . \\ . \\ i_1^2 \\ i_2^2 \\ i_1^1 \end{array} \tag{53}$$

The column with index i_1^{λ} (=1) corresponds, as usual, with the irreducible polynomial which defines the primitive 2^{λ}-th root of unity ζ in some extension field of $GF(q)$ and also with the cyclotomic coset $C_1 = \{1, q, ..., q^{r_\lambda - 1}\}$. The column with index i_1^1 corresponds with the irreducible polynomial $P_{i_1^1}(x) := \Phi_2(x) = x + 1$ which defines the only element of the cyclotomic coset $C_{2^{\lambda-1}} = \{2^{\lambda-1}\} = \{-1\}$. In the first row of M the integers r_b satisfy $r_b = 2^{b-2} r_2$, $2 \le b \le \lambda$, and $r_1 = r_2 = 1$ (cf. [4, Lemma 58 (ii) and its proof]). The integers in the last column are equal to 1 if the value of the row index i_j^k is even, and they are equal to -1 if this value is odd. One can see this by using the definition of the matrix elements $\mu_{i,j} = -\frac{m_j}{m_{ij}} p_{ij,1}$ where m_a is the degree of the irreducible polynomial $P_a(x)$ while $p_{a,1}$ denotes the coefficient of the term $x^{m_a - 1}$ in that polynomial. All matrix elements are in $GF(q)$.

Example 10

We continue the case $p = 2$, $\lambda = 4$, $q = 5$ which was studied already in [4, Example 60]. With the facts found and derived in [4] we are able to construct the matrix *M* completely. For the index set *S* we found

$$0, i_1^4, i_2^4, i_1^3, i_2^3, i_1^2, i_2^2, i_1^1 = 0, 1, 3, 2, 6, 4, 12, 8 ,$$

which shows that $\kappa_1 = 1$, $\kappa_2 = \kappa_3 = \kappa_4 = 2$, as should be according to eq. (32).
The corresponding irreducible polynomials are

$P_0(x) = x-1$, $P_1(x) = x^4+2$, $P_3(x) = x^4+3$, $P_2(x) = x^2+2$, $P_6(x) = x^2+3$, $P_4(x) = x+2$, $P_{12}(x) = x+3$ and $P_8(x) = x+1$.

By using the expression $\mu_{j,i} = -\frac{m_i}{m_{ij}} p_{ij,1}$ for its elements, we are now able to construct the matrix *M*. We find

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 3 & 2 & 6 & 4 & 12 & 8 \end{matrix} \\ \begin{pmatrix} 1 & 4 & 4 & 2 & 2 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & -2 & -3 & -1 \\ 1 & 0 & 0 & 0 & 0 & -3 & -2 & -1 \\ 1 & 0 & 0 & -4 & -6 & -1 & -1 & 1 \\ 1 & 0 & 0 & -6 & -4 & -1 & -1 & 1 \\ 1 & -8 & -12 & -2 & -2 & 1 & 1 & 1 \\ 1 & -12 & -8 & -2 & -2 & 1 & 1 & 1 \\ 1 & -4 & -4 & 2 & 2 & 1 & 1 & 1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 3 \\ 2 \\ 6 \\ 4 \\ 12 \\ 8 \end{matrix}$$

With the help of the weight vector (1, 4, 4, 2, 2, 1, 1, 1) (i.e. the vector containing the sizes of the cyclotomic cosets), one can check the various orthogonality relations of *M*, as stated in [4, Theorem 28]. □

Case B

The second class consists of *GR*-codes with $n = 2^2$, $q = 1+4l$, l even, (cf. (33)).

The cyclotomic cosets mod 4 are $C_0 = \{0\}$, $C_1 = \{1\}$, $C_2 = \{2\}$, $C_3 = \{3\}$, and so $m_0 = m_1 = m_2 = m_3 = 1$. The corresponding irreducible polynomials are $P_0(x) = x-1$, $P_1(x) = x-\alpha$, $P_2(x) = x-\beta$, $P_3(x) = x+1$, where $\alpha := \zeta^1$ and $\beta := \zeta^3$, if ζ is a primitive 4^{th} root of 1 in $GF(q)$. Notice that $(x-\alpha)(x-\beta) = x^2+1 = \Phi_2(x)$. By defining $i_1^2 = 1$, $i_2^2 = 3$, $i_1^1 = 2$, and by putting $r_1 = r_2 = 1$, the matrix M is also of the form (53) with $\lambda = 2$:

$$M = \begin{array}{c} \begin{matrix} 0 & i_1^2 & i_2^2 & i_1^1 \end{matrix} \\ \begin{pmatrix} 1 & r_2 & r_2 & r_1 \\ 1 & \alpha & \beta & -1 \\ 1 & \beta & \alpha & -1 \\ 1 & -r_2 & -r_2 & 1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ i_1^2 \\ i_2^2 \\ i_1^1 \end{matrix}. \qquad (54)$$

When taking as specific example q = 17, we have $\alpha = 4$ and $\beta = -4$. All orthogonality relations of [4, Theorem 28] are satisfied, e.g. column i_1^2 is orthogonal to itself, since $1+16+16 = 34 = 0$ in $GF(17)$, while the innerproduct of columns i_1^2 and i_2^2 equals $1-16-16+1 = -30 = 4 = n$.
Another specific example is $q = 9$. In this case we have $\alpha = \zeta$ and $\beta = -\zeta$, where ζ is again defined as a primitive 4^{th} root of unity, this time in $GF(9)$. Since $\zeta^2 = -1$, the orthogonality relations hold again. It can easily be seen that these relations hold in general for all relevant values of q, for the same reason.

Case C
The third class consists of the GR-codes with $n = 2^\lambda$, $\lambda \geq 3$, $q = -1+4l$, l odd (cf. (34)). The matrix M is now a $(2\lambda-1)\times(2\lambda-1)$-matrix of the form

$$M = \begin{array}{c} \begin{array}{ccccccccccccc} 0 & i_1^\lambda & i_2^\lambda & i_1^{\lambda-1} & i_2^{\lambda-1} & . & . & i_1^3 & i_2^3 & i_1^2 & i_1^1 & \end{array} \\ \begin{pmatrix} 1 & r_\lambda & r_\lambda & r_{\lambda-1} & r_{\lambda-1} & . & . & r_3 & r_3 & r_2 & r_1 \\ 1 & 0 & 0 & . & . & . & . & 2^{3-\lambda}\alpha & 2^{3-\lambda}\beta & 0 & -1 \\ 1 & 0 & 0 & . & . & . & . & 2^{3-\lambda}\beta & 2^{3-\lambda}\alpha & 0 & -1 \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ 1 & \alpha & \beta & . & . & . & . & . & . & . & 1 \\ 1 & \beta & \alpha & . & . & . & . & . & . & . & 1 \\ 1 & 0 & 0 & . & . & . & . & . & . & . & 1 \\ 1 & -r_\lambda & -r_\lambda & . & . & . & . & . & . & . & 1 \end{pmatrix} \end{array} \begin{array}{c} 0 \\ i_1^\lambda \\ i_2^\lambda \\ i_1^{\lambda-1} \\ i_2^{\lambda-1} \\ . \\ . \\ i_1^3 \\ i_2^3 \\ i_1^2 \\ i_1^1 \end{array} \qquad (55)$$

The column with index $i_1^\lambda (=1)$ corresponds (again) with the irreducible polynomial which defines the 2^λ-th root of unity in some extension field of $GF(q)$ and also with the cyclotomic coset $C_1 = \{1, q, ..., q^{r_\lambda - 1}\}$. The column with index i_1^1 corresponds with the polynomial $P_{i_1^1}(x) := \Phi_2(x) = x+1$ and also with the cyclotomic coset $C_{2^{\lambda-1}} = \{2^{\lambda-1}\} = \{-1\}$, while the column with index i_1^2 corresponds with the irreducible polynomial $P_{i_1^2}(x) := \Phi_4(x) = x^2+1$ and with the cyclotomic coset $C_{2^{\lambda-2}} = \{2^{\lambda-2}, 2^{\lambda-2}q\}$. Consequently, we have $i_1^1 = 2^{\lambda-1}$, $i_1^2 = 2^{\lambda-2}$, $r_1 = 1$ and $r_2 = 2$. We also know (cf. [4, Lemma 58 (iii) and its proof]) that $r_b = 2^{b-3} r_3$, with $r_3 = 2$.

Example 11

Take $\lambda = 3$ and $q = 11$. The cyclotomic cosets mod 8 with respect to 11 are $C_0 = \{0\}$, $C_1 = \{1,3\}$, $C_2 = \{2,6\}$, $C_4 = \{4\}$, $C_5 = \{5,7\}$, so $m_0 = m_4 = 1$ and $m_1 = m_2 = m_5 = 2$. The irreducible polynomials in $GF(11)[x]$ are $P_0(x) = x - 1$, $P_1(x) = x^2 + 3x - 1$, $P_5(x) = x^2 - 3x + 1$, $P_2(x) = x^2 + 1$ and $P_4(x) = x + 1$.

Notice that $P_1(x)P_5(x) = x^4 + 1 = \Phi_8(x)$ and $P_2(x) = \Phi_4(x)$. Using these facts, we find for M the following matrix

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 5 & 2 & 4 \end{matrix} \\ \begin{pmatrix} 1 & 2 & 2 & 2 & 1 \\ 1 & -3 & 3 & 0 & -1 \\ 1 & 3 & -3 & 0 & -1 \\ 1 & 0 & 0 & -2 & 1 \\ 1 & -2 & -2 & 2 & 1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 5 \\ 2 \\ 4 \end{matrix}.$$

□

Case D

The fourth class consists of *GR*-codes with $n = 2^3$, $q = -1 + 4l$, l even (cf. (35)).
First we give an example for $\lambda > 3$.

Example 12

Take $p = 2$, $\lambda = 5$ and $q = 7$ (cf. again [4, Example 60]).
In [4] we found for the index set *S*

$$0, i_1^5, i_2^5, i_3^5, i_4^5, i_1^4, i_2^4, i_3^4, i_4^4, i_1^3, i_2^3, i_1^2, i_1^1 = 0,1,9,3,11,2,18,6,22,4,12,8,16,$$

which shows that indeed $\kappa_1 = \kappa_2 = 1$ and $\kappa_3 = 2$, and that $\kappa_4 = \kappa_5 = 4$ (cf. eq. (35)). The irreducible polynomials corresponding to the respective indices are $P_0(x) = x - 1$ and

$$P_1(x) = x^4 - x^2 - 1,\ P_9(x) = x^4 + x^2 - 1,\ P_3(x) = x^4 - 4x^2 - 1,\ P_{11}(x) = x^4 + 4x^2 - 1,$$
$$P_2(x) = x^2 - x - 1,\ P_{18}(x) = x^2 + x - 1,\ P_6(x) = x^2 - 4x - 1,\ P_{22}(x) = x^2 + 4x - 1,$$
$$P_4(x) = x^2 + 4x + 1,\ P_{12}(x) = x^2 - 4x + 1,\ P_8(x) = x^2 + 1,\ P_{16}(x) = x + 1.$$

□

The above example confirms the result that if $p = 2$ and $q = -1 + 4l$, l even, κ_λ can only be equal to 2 for $\lambda = 3$. In general, we have that for $n = 2^3$ and $q = -1 + 4l$, l even, the cyclotomic cosets with respect to q are $C_0 = \{0\}$, $C_1 = \{1,7\}$, $C_2 = \{2,6\}$, $C_3 = \{3,5\}$ and $C_4 = \{4\}$. So, $m_0 = m_4 = 1$ and $m_1 = m_2 = m_3 = 2$. The corresponding irreducible

polynomials are $P_0(x) = x-1$, $P_1(x) = x^2 + \alpha x + 1$, $P_2(x) = x^2 + 1$, $P_3(x) = x^2 - \alpha x + 1$ and $P_4(x) = x+1$, where $\alpha \in GF(q)$ is defined by $\alpha^2 = 2$.

By using the expression $\mu_{j,i} = -\frac{m_i}{m_{ij}} p_{ij,1}$ for the matrix elements of the matrix M, we derive the following matrix

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 3 & 2 & 4 \end{matrix} \\ \begin{pmatrix} 1 & 2 & 2 & 2 & 1 \\ 1 & -\alpha & \alpha & 0 & -1 \\ 1 & \alpha & -\alpha & 0 & -1 \\ 1 & 0 & 0 & -2 & 1 \\ 1 & -2 & -2 & 2 & 1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 3 \\ 2 \\ 4 \end{matrix}. \qquad (56)$$

One can easily verify the orthogonality relations for this matrix *M*. Remark that the matrix at the end of C is not a special case of (56), since $3^2 = -2 \neq 2$ in $GF(11)$. As a consequence the inner product of the columns with index 1 and with index 5 in that matrix is equal to $1.2.2 + 2.(-3).3 + 2.3.(-3) + 2.0.0 + 1.(-2).(-2) = 5 (= m_1 n = 2.8)$ in $GF(11)$, while these columns are orthogonal to themselves, since e.g. $1.2^2 + 2.(-3)^2 + 2.3^2 + 2.0^2 + 1.(-2)^2 = 0$. On the other hand, the inner product of columns 1 and 3 in (56) equals $1.2.2 + 2.(-\alpha).(\alpha) + 2.(\alpha).(-\alpha) + 2.0.0 + 1.(-2).(-2) = 8 - 4\alpha^2 = 0$, and so they are orthogonal, while the inner product of such a column with itself equals $16 = 2.8 = m_i n$, $i \in \{1,3\}$, e.g. $1.2^2 + 2.(-\alpha)^2 + 2.\alpha^2 + 2.0^2 + +1.(-2)^2 = 8 + 4\alpha^2 = 16$.

6. Idempotent generators for *DGQR*-codes

An essential element in the construction of idempotent generators of *GQR*-codes $C^i_{p^\lambda,q,2}$ as applied in the previous sections is the fact that U_{p^λ} is a cyclic group. This enhances that its subgroup Q_{p^λ} of quadratic residues is also cyclic and that it has an index 2 with respect to U_{p^λ}. In [3] we saw that there exists another family of cyclic groups U_n, i.e. when $n = 2p^\lambda$, with *p* an odd prime. In this section we shall develop a similar construction method for idempotent generators for *GR*-codes of type $C^i_{2p^\lambda,q,2}$ which are based on U_{2p^λ}. We shall call such codes *double generalized quadratic residue codes*, or briefly *DGQR-codes*), since the underlying group *K* is equal to the group of quadratic residues mod $2p^\lambda$, similar to the case of generalized quadratic residue codes.

We take for p an odd prime and for q an odd prime power with $(p,q)=1$ and we assume that q is a generator of the group Q_{2p^λ}. This group will also be indicated by just Q when it is clear from the context that we are dealing with quadratic residues mod $2p^\lambda$.
As a consequence, we have again (cf. Section 3) that $H :=< q >= K = Q,\ s = 1,$ $\kappa = st = 2$, while now $r := \mathrm{ord}_n(q) = \varphi(n)/2$ with $n = 2p^\lambda$.

For reasons of convenience, we first consider the case $\lambda = 1$, like in Section 3. Then we have $\varphi(n) = \varphi(2p) = p-1$, and so

$$r = (p-1)/2. \tag{57}$$

The cyclotomic polynomial $\Phi_{2p}(x)$ can be factorized as

$$\Phi_{2p}(x) = \Phi_1(x)\Phi_2(x)\Phi_p(x)\Phi_{2p}(x) = (x-1)(x+1)\Phi_p(x)\Phi_{2p}(x). \tag{58}$$

Furthermore, the nonzero cyclotomic cosets mod $2p$ are $C_1 = \{1, q, ..., q^{r-1}\}$, $C_a = \{a, aq, ..., aq^{r-1}\}$, $C_2 = \{2, 2q, ..., 2q^{r-1}\}$, $C_{2a} = \{2a, 2aq, ..., 2aq^{r-1}\}$ and $C_p = \{p\}$, for some odd integer *a.* Because q generates Q_{2p}, we have $C_1 = Q_{2p}$.
The cosets C_1 and C_a correspond to the two irreducible polynomials of degree $r-1$ contained in $\Phi_{2p}(x)$, while C_2 and C_{2a} correspond to the two irreducible polynomials of degree $r-1$ contained in $\Phi_p(x)$, all over the field $GF(q)$. The cyclotomic coset C_p corresponds to $\Phi_2(x) = x+1$. Like in Sections 3 and 4, we can take $a = -1$ if and only if $p = -1 \mod 4$.
Because the total number of cyclotomic cosets is six, the matrix M is a 6×6-matrix.

For $p = \pm 1 \mod 8$, we have that $2 \in Q_p$, so $C_{1+p} = C_2$ and $C_{a+p} = C_{2a}$ (cf.). Hence, in this case the rows and columns of M can be labeled by the indices $0, 1, a, 2, 2a, p$. Using the definition of the matrix elements $\mu_{j,i}$ it appears that this matrix has the form

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & a & 2 & 2a & p \end{matrix} \\ \begin{pmatrix} 1 & r & r & r & r & 1 \\ 1 & \gamma & \delta & -\gamma & -\delta & -1 \\ 1 & \delta & \gamma & -\delta & -\gamma & -1 \\ 1 & -\gamma & -\delta & -\gamma & -\delta & 1 \\ 1 & -\delta & -\gamma & -\delta & -\gamma & 1 \\ 1 & -r & -r & r & r & -1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ a \\ 2 \\ 2a \\ p \end{matrix}, \qquad r, \gamma, \delta \in GF(q). \tag{59}$$

The mutual dependence of the matrix elements is mainly due to the properties $P_2(x) = P_{1+p}(x) = (-1)^r P_1(-x)$ and $P_{2a}(x) = P_{a+p}(x) = (-1)^r P_a(-x)$ as one can prove easily (cf. also [4, Section 6]), and hence $p_{2,1} = -p_{1,1}$ and $p_{2a,1} = -p_{a,1}$.
The matrix elements $\mu_{p,i}$, $i \in \{1, a, 2, , 2a, p\}$ follow from the definition (cf. [4, eq. (41)])

$\mu_{j,i} = -\frac{m_i}{m_{ij}} p_{ij,1}$ and from the values $p_{0,1} = -1$ and $p_{p,1} = 1$ as coefficients in the polynomials $P_0(x) = x - 1$ and $P_p(x) = x + 1$, respectively. As for the matrix elements $\mu_{j,p} = -p_{jp,1}$, these are equal to 1 if j has an even value (0, 2 or $2a$), and to -1 if j has an odd value (1, a or p). After putting $\mu_{1,1} := \gamma$ and $\mu_{a,1} := \delta$, the remaining matrix elements follow from their definition, e.g. $\mu_{1,2} = -p_{2,1} = p_{1,1} = -\mu_{1,1} = -\gamma$ and $\mu_{1,2a} = -p_{2a,1} = p_{a,1} = -\mu_{a,1} = -\delta$. For the elements $\mu_{j,i}$, $i, j \in \{2, 2a\}$ we also use the fact that $4 \in C_2$ if and only if $2 \in Q_p = C_1$, which is the case if and only if $p = \pm 1 \bmod 8$. Since we assumed $p = \pm 1 \bmod 8$, it follows e.g. that $\mu_{2,2} = -p_{2,1} = p_{1,1} = -\mu_{1,1} = -\gamma$.

For $p = \pm 3 \bmod 8$, we have $2 \notin Q_p$, and so $2 \in C_a'$. It follows that $C_{1+p} = C_{2a}$, $C_{a+p} = C_2$. According to our labeling convention in [4], the indices of the rows and columns of M are $0, 1, a, 2a, 2, p$, and the matrix itself appears to have the form

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & a & 2a & 2 & p \end{matrix} \\ \begin{pmatrix} 1 & r & r & r & r & 1 \\ 1 & \gamma & \delta & -\gamma & -\delta & -1 \\ 1 & \delta & \gamma & -\delta & -\gamma & -1 \\ 1 & -\gamma & -\delta & -\gamma & -\delta & 1 \\ 1 & -\delta & -\gamma & -\delta & -\gamma & 1 \\ 1 & -r & -r & r & r & -1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ a \\ 2a \\ 2 \\ p \end{matrix}, \qquad r, \gamma, \delta \in GF(q). \qquad (60)$$

Remark 13
The matrices (59) and (60) are completely identical. This suggests that distinguishing between the cases $2 \in Q_p$ and $2 \notin Q_p$ is not necessary. Therefore, in the general case of code length $n = p^\lambda$, $\lambda \geq 1$, we shall avoid this distinction.

Next, we shall determine explicit expressions for the values of γ and δ in (59) and (60), in terms of p and q.

(i) $p = 1 \mod 4$

In this case -1 is a quadratic residue and so $-1 \in C_1$, $a \neq -1$. Since q is odd, the relations of [4, Theorem 28 (i)] give

$$1 - \gamma - \delta = 0, \tag{61}$$

$$r + \gamma^2 + \delta^2 = p, \tag{62}$$

$$r + 2\gamma\delta = 0. \tag{63}$$

Eqs. (62) and (63) follow from the orthonormality of row 1 and columns 1 and a, respectively. Eq. (61) follows from the orthogonality of row 0 and column 2 in (59) if $p = 1 \mod 8$ and of row 0 and column 2 in (60) if $p = -3 \mod 8$.

Solving δ from (61) and substituting in (62) or in (63) yields the equation

$$(2\gamma - 1)^2 = p, \tag{64}$$

resulting in

$$\gamma = \frac{1 + \sqrt{p}}{2}, \quad \delta = \frac{1 - \sqrt{p}}{2}. \tag{65}$$

(ii) $p = -1 \mod 4$

Now, -1 is not a quadratic residue, and so we can put $a = -1$.

From [4, Theorem 28 (i)] we obtain

$$1 - \gamma - \delta = 0, \tag{66}$$

$$r + \gamma^2 + \delta^2 = 0, \tag{67}$$

$$r + 2\gamma\delta = p. \tag{68}$$

From these equations it follows easily that

$$\gamma = \frac{1 + \sqrt{-p}}{2}, \quad \delta = \frac{1 - \sqrt{-p}}{2}. \tag{69}$$

We conclude that the primitive idempotent generators of the cyclic codes corresponding to columns 1 and a of the matrix M are

$$\theta_1(x) = (2p)^{-1}(r(1 - x^p) + \gamma \sum_{i \in C_1} (x^i - x^{2i}) + \delta \sum_{i \in C_a} (x^i - x^{2i})), \tag{70}$$

$$\theta_a(x) = (2p)^{-1}(r(1-x^p) + \delta\sum_{i\in C_1}(x^i - x^{2i}) + \gamma\sum_{i\in C_a}(x^i - x^{2i})). \qquad (71)$$

with γ and δ from (65) if $p = 1 \bmod 4$, and from (69) if $p = -1 \bmod 4$.
Finally, the idempotent generators of the *DGQR*-codes $C^i_{2p,q,2}$, $i \in \{1, a\}$, can be written as

$$\vartheta_i(x) = 1 - \theta_i(x), \quad i \in \{1, a\}. \qquad (72)$$

Example 14
Take $p = 5 (= -3) \bmod 8$. The group $U_{10} = \{1,3,7,9\}$ with $Q_{10} = \{1,9\}$ as subgroup of quadratic residues mod 10 which are prime to 10. So, $q = 9$ is a prime power which generates Q_{10} with $r := \mathrm{ord}_{10}(9) = 2$.
The cyclotomic cosets mod 10 with respect to q are $C_0 = \{0\}$, $C_1 = \{1,9\}$, $C_3 = \{3,7\}$, $C_2 = \{2,8\}$, $C_6 = \{6,4\}$ and $C_5 = \{5\}$.
Since 5 = 1 mod 4, we are in case (i). Hence, by applying (59) we have in $GF(9)$

$$\gamma = \frac{1+\sqrt{5}}{2} = \frac{1+\sqrt{2}}{2} = \frac{1+(\xi-1)}{2} = -\xi, \quad \delta = \frac{1-\sqrt{5}}{2} = 1+\xi,$$

where ξ is a zero of $x^2 + x - 1 = 0$ and hence satisfies $\xi^2 = -\xi + 1$.

With (70) and (71) we find the following idempotent generators corresponding to the columns indexed by 1 and 3(=*a*).

$$\theta_1(x) = -1 + x^5 - \xi(x + x^9 - x^2 - x^8) + (1+\xi)(x^3 + x^7 - x^6 - x^4),$$

$$\theta_3(x) = -1 + x^5 + (1+\xi)(x + x^9 - x^2 - x^8) - \xi(x^3 + x^7 - x^6 - x^4).$$

The idempotent generators of the two *DGQR*-codes $C^i_{10,9,2}$, $i \in \{1,3\}$, are obtained by $\vartheta_i(x) = 1 - \theta_i(x)$.

We shall also establish the relationship between the cyclotomic cosets and the irreducible polynomials in a similar way as in [4, Example 40]. We introduce the following irreducible polynomials
over $GF(9)$: $P_0(x) = x - 1$, $P_1(x) = x^2 + \xi x + 1$, $P_2(x) = x^2 + (\xi+1)x + 1$, $P_3(x) = x^2 - (\xi+1)x + 1$, $P_6(x) = x^2 - \xi x + 1$ and $P_5(x) = x + 1$. One can easily show that these polynomials correspond to the cyclotomic cosets C_0, C_1, C_2, C_3, C_6 and C_5, respectively. Moreover, one can also verify that the cyclotomic polynomials

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ and $\Phi_{10}(x) = \Phi_5(-x) = x^4 - x^3 + x^2 - x + 1$ factorize as $\Phi_{10}(x) = P_1(x)P_3(x)$ and $\Phi_5(x) = P_2(x)P_6(x)$.
From the coefficients $p_{i,1}$, $i \in \{0,1,2,3,6,5\}$, we now derive the complete matrix M

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 3 & 6 & 2 & 5 \end{matrix} \\ \begin{pmatrix} 1 & 2 & 2 & 2 & 2 & 1 \\ 1 & -\xi & \xi+1 & \xi & -\xi-1 & -1 \\ 1 & \xi+1 & -\xi & -\xi+1 & \xi & -1 \\ 1 & \xi & -\xi-1 & -\xi+1 & \xi & 1 \\ 1 & -\xi-1 & \xi & \xi & -\xi-1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 3 \\ 6 \\ 2 \\ 5 \end{matrix}$$

As one immediately can verify, the second and third column, indexed by 1 and 3, contain the very same coefficients as we found by applying (60) which was derived without using the explicit form of the irreducible polynomials. The only knowledge our method does not provide us with, is which one of the constructed idempotent generators corresponds to which polynomial. The whole matrix is conform the general structure of M for $p = -3$ as shown in (60). □

Example 15

Now we take $p = 7(= -1) \bmod 8$. The group $U_{14} = \{1,3,5,9,11,13\}$ has $Q_{14} = \{1,9,11\}$ as subgroup of quadratic residues. So, 9 and 11 are prime powers which generate Q_{14} with $r := \mathrm{ord}_{14}(9) = \mathrm{ord}_{14}(11) = 3$. Take $q = 9$. The cyclotomic cosets mod 14 with respect to q are $C_0 = \{0\}$, $C_1 = \{1,9,11\}$, $C_3 = \{3,13,5\}$, $C_2 = \{2,4,8\}$, $C_6 = \{6,12,10\}$ and $C_7 = \{7\}$.
Since $7 = -1 \bmod 4$, we apply (69), yielding in $GF(9)$

$$\gamma = \frac{1+\sqrt{-7}}{2},\ \delta = \frac{1-\sqrt{-7}}{2}.$$

Let $GF(9)$ be defined as the extension of $GF(3)$ by ξ which satisfies $\xi^2 = -\xi + 1$. Then $\xi^4 = -1$, and hence $\sqrt{-7} = \sqrt{-1} = \xi^2$ and so $\gamma = -\xi^3$ and $\delta = -\xi$. With expressions (70) and (71) we find the following primitive idempotent generators corresponding to the columns with index 1 and 3(=a)

$$\theta_1(x) = \xi^3(x + x^9 + x^{11} - x^2 - x^4 - x^8) + \xi(x^3 + x^5 + x^{13} - x^6 - x^{10} - x^{12}),$$

$$\theta_3(x) = \xi(x + x^9 + x^{11} - x^2 - x^4 - x^8) + \xi^3(x^3 + x^5 + x^{13} - x^6 - x^{10} - x^{12}).$$

The irreducible polynomials which correspond to the cyclotomic cosets mod 14 are $P_0(x) = x-1$, $P_1(x) = x^3 + \xi^3 x^2 + \xi x + 1$, $P_3(x) = x^3 + \xi x^2 + \xi^3 x^2 + 1$, $P_2(x) = x^3 - \xi^3 x^2 + \xi x - 1$, $P_6(x) = x^3 - \xi x^2 + \xi^3 x - 1$ and $P_7(x) = x + 1$. The cyclotomic polynomials $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $\Phi_{14}(x) = x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$ factorize as $\Phi_{14}(x) = P_1(x)P_3(x)$ and $\Phi_7(x) = P_2(x)P_6(x)$. The coefficients $p_{i,1}$, $i \in \{0,1,3,2,6,7\}$, of the irreducible polynomials, give rise to the matrix

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 3 & 2 & 6 & 7 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & -\xi^3 & -\xi & \xi^3 & \xi & -1 \\ 1 & -\xi & -\xi^3 & \xi & \xi^3 & -1 \\ 1 & \xi^3 & \xi & \xi^3 & \xi & 1 \\ 1 & \xi & \xi^3 & \xi & \xi^3 & 1 \\ 1 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 3 \\ 2 \\ 6 \\ 7 \end{matrix}$$

which is indeed an illustration of the general form (59). □

Next, we study the general case where λ is arbitrary integer ≥ 1. From [4,(62)] it follows that the rows and columns of the matrix M for codes of length $2p^\lambda$ over $GF(q)$, with $t = 2$, are labeled by

$$0, i_1^\lambda, i_2^\lambda, i_1^{\lambda-1}, i_2^{\lambda-1}, ..., i_1^1, i_2^1, i_3^\lambda, i_4^\lambda, i_3^{\lambda-1}, i_4^{\lambda-1}, ..., i_3^1, i_4^1, p^\lambda. \tag{73}$$

So, the size of M is $(4\lambda+2)\times(4\lambda+2)$. Similarly as in the case of the matrix M for codes of length p^λ over $GF(q)$ with $t = 2$ (cf. Section 2), and also similar to the case $\lambda = 1$ in the first part of this section, we put $i_1^\lambda = 1$, $i_2^\lambda = a$, $i_3^\lambda = 1 + p^\lambda$ and $i_4^\lambda = a + p^\lambda$. Here, we assume that we have cyclotomic cosets $C_{i_1^\lambda} = C_1 = \{1, q, ..., q^{r_\lambda - 1}\}$, $C_{i_2^\lambda} = C_a = \{a, aq, ..., aq^{r_\lambda - 1}\}$, $C_{i_3^\lambda} = C_{1+p^\lambda} = \{1 + p^\lambda, q + p^\lambda, ..., q^{r_\lambda - 1} + p^\lambda\}$, and $C_{i_4^\lambda} = C_{a+p^\lambda} = \{a + p^\lambda, aq + p^\lambda, ..., aq^{r_\lambda - 1} + p^\lambda\}$. In general the cyclotomic cosets $\neq C_0, C_{p^\lambda}$ can be labeled as $C_{p^{\lambda-b}}$, $C_{ap^{\lambda-b}}$, $C_{p^{\lambda-b}+p^\lambda}$ and $C_{ap^{\lambda-b}+p^\lambda}$ (we omit the enumeration of the elements in the various cosets), for $1 \leq b \leq \lambda$. The size of all these cosets equals

$$r_b = rp^{b-\lambda}. \tag{74}$$

It is obvious that the cyclotomic coset C_1 coincides with Q_{2p^λ}, C_a with $N_{2p^\lambda}(=U_{2p^\lambda} \setminus Q_{2p^\lambda})$, C_{1+p^λ} with $p^\lambda + Q_{2p^\lambda}$ and C_{a+p^λ} with $p^\lambda + N_{2p^\lambda}$.

The following lemma, stating a relationship between the groups of quadratic residues Q_{2p^λ} and Q_{p^λ}, appears to be useful for the derivation of the general form of the matrix *M*.

Lemma 16

Let p be an odd prime and q be an odd prime power, such that $(p,q)=1$. *Let* $Q_{2p^\lambda} \subset U_{2p^\lambda}$ *be the group of quadratic residues mod* $2p^\lambda$ *in* U_{2p^λ}, *and* $Q_{p^\lambda} \subset U_{p^\lambda}$ *be the group of quadratic residues mod* p^λ, $\lambda \geq 1$. *Let furthermore* $N_{2p^\lambda} \subset U_{2p^\lambda}$ *be the set of non-quadratic residues in* U_{2p^λ}.

(i) *The mapping* $f : Q_{p^\lambda} \to U_{2p^\lambda}$, $f(c)=c$ *if c is odd, and* $f(c)=c+p^\lambda$ *if a is even, defines a one-to-one mapping of* Q_{p^λ} *onto* Q_{2p^λ};

(ii) *One of the sets* $p^\lambda + Q_{2p^\lambda}$ *and* $p^\lambda + N_{2p^\lambda}$ *contains the even quadratic residues mod* $2p^\lambda$, *while the other contains the even non-quadratic residues*;

Proof

For any $c \in Q_{p^\lambda}$ we have $c = b^2 + kp^\lambda$, $b \in U_{p^\lambda}$, for some integer k.

(i) Let c be odd. If b is odd, then k is even, and so $c \in Q_{2p^\lambda}$.

If b is even, then k is odd. We write $(b+p^\lambda)^2 = b^2 + p^{2\lambda} = c + p^\lambda(p^\lambda - k) \mod 2p^\lambda$. Since $p^\lambda - k$ is even, we may conclude that again $c \in Q_{2p^\lambda}$.

Let c be even. If b is even, then k is even, and so $c \in Q_{2p^\lambda}$.

If b is odd, then k is odd. We write $(b+p^\lambda)^2 = b^2 + p^{2\lambda} = c + p^\lambda(p^\lambda - k) \mod 2p^\lambda$, from which it follows that again $c \in Q_{2p^\lambda}$, since $p^\lambda - k$ is even.

It is obvious that f is an injective mapping. We know that $\left| Q_{2p^\lambda} \right| = \left| Q_{p^\lambda} \right| = \varphi(p^\lambda)$, and therefore f is also onto.

(ii) Take $c \in Q_{2p^\lambda}$, then $c = b^2 \mod 2p^\lambda$, with b odd. We can write $c + p^\lambda = b^2 + p^\lambda = (b+p^\lambda)^2 - p^\lambda(p^\lambda + 2b - 1)$, and hence $(c+p)^2 = (b+p^\lambda)^2 \mod 2p^\lambda$, and $b + p^\lambda$ is even.

The proof for $p^\lambda + N_{2p^\lambda}$ is similar. □

With respect to the conventions for the labeling of rows and columns, the matrix M takes in general the following form.

$$
\mathrm{M} = \begin{array}{c}
\begin{array}{ccccccccccccc} 0 & 1 & a & . & . & p^{\lambda-1} & ap^{\lambda-1} & 1+p^{\lambda} & a+p^{\lambda} & . & . & p^{\lambda-1}+p^{\lambda} & ap^{\lambda-1}+p^{\lambda} & p^{\lambda} \end{array} \\
\begin{pmatrix}
1 & r_{\lambda} & r_{\lambda} & . & . & r_1 & r_1 & r_{\lambda} & r_{\lambda} & . & . & r_1 & r_1 & 1 \\
1 & 0 & 0 & . & . & p^{1-\lambda}\gamma & p^{1-\lambda}\delta & 0 & 0 & . & . & -p^{1-\lambda}\gamma & -p^{1-\lambda}\delta & -1 \\
1 & 0 & 0 & . & . & p^{1-\lambda}\delta & p^{1-\lambda}\gamma & 0 & 0 & . & . & -p^{1-\lambda}\delta & -p^{1-\lambda}\gamma & -1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . \\
1 & 0 & 0 & . & . & . & . & 0 & 0 & . & . & . & . & -1 \\
1 & \gamma & \delta & . & . & . & . & . & . & . & . & . & . & -1 \\
1 & \delta & \gamma & . & . & . & . & . & . & . & . & . & . & -1 \\
1 & 0 & 0 & . & . & . & . & 0 & 0 & . & . & . & . & 1 \\
1 & 0 & 0 & . & . & . & . & 0 & 0 & . & . & . & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . \\
1 & 0 & 0 & . & . & . & . & . & . & . & . & . & . & 1 \\
1 & -\gamma & -\delta & . & . & . & . & . & . & . & . & . & . & 1 \\
1 & -\delta & -\gamma & . & . & . & . & . & . & . & . & . & . & 1 \\
1 & -r_{\lambda} & -r_{\lambda} & . & . & -r_1 & -r_1 & r_{\lambda} & r_{\lambda} & . & . & r_1 & r_1 & -1
\end{pmatrix}
\end{array}
\tag{75}
$$

with $\gamma, \delta \in GF(q)$.

We did not fill in the remaining open positions in the matrix *M*, because we don't need these for the computation of the primitive idempotents which correspond to columns 1 and *a*. The zeros in these columns stem from the fact that the indices i_1^b and i_2^b indicate the irreducible polynomials $P_1(x^{p^{b-1}})$ and $P_a(x^{p^{b-1}})$, for any *b* with $1 \le b \le \lambda$. In these polynomials the coefficients $p_{i_1^b,1}$ and $p_{i_a^b,1}$ are equal to zero for all *b* with $1 < b \le \lambda$.

Only for $\lambda = 1$ we shall fill in the vacancies. From Lemma 16 (ii) it follows that $C_{1+p}C_{1+p} = C_{1+p}$ and $C_{a+p}C_{a+p} = C_{1+p}$. Hence, $\mu_{1+p,1+p} = -p_{1+p,1} = p_{1,1} = -\mu_{1,1} = -\gamma$ and $\mu_{a+p,a+p} = -p_{1+p,1} = p_{1,1} = -\gamma$. Also $C_{1+p,a+p} = C_{a+p}$ and so $\mu_{1+p,a+p} = \mu_{a+p,1+p} = -p_{a+p,1} = p_{a,1} = -\mu_{a,1} = -\delta$. This proves Remark 13.

Next, we shall state and prove the theorem which will enable us to write explicit expressions for the primitive idempotent generators for codes belonging to columns 1 and *a*, and consequently for all *DGQR*-codes.

Theorem 17

Let p be some odd prime and q some odd prime power with $(p,q)=1$ *which satisfy conditions* (43) *and* (44)*, and let q be a generator of the group* Q_{2p^λ} *of quadratic residues mod* $2p^\lambda$*. Let furthermore M be the matrix for codes of length* $2p^\lambda$*,* $\lambda \geq 1$*, over* $GF(q)$*, with t = 2, and let a be some integer from* $U_{2p^\lambda} \setminus Q_{2p^\lambda}$*. Then the two primitive idempotent generators which correspond to the columns 1 and a of the matrix M can for* $p=1 \mod 4$ *be written as*

$$\theta_1(x)=\frac{1-x^{p^\lambda}}{4p}[(p-1)+(1+\sqrt{p})\sum_{i\in Q_p} x^{ip^{\lambda-1}}+(1-\sqrt{p})\sum_{i\in Q_p} x^{aip^{\lambda-1}}],$$

$$\theta_a(x)=\frac{1-x^{p^\lambda}}{4p}[(p-1)+(1-\sqrt{p})\sum_{i\in Q_p} x^{ip^{\lambda-1}}+(1+\sqrt{p})\sum_{i\in Q_p} x^{aip^{\lambda-1}}],$$

and for $p=-1 \mod 4$

$$\theta_1(x)=\frac{1-x^{p^\lambda}}{4p}[(p-1)+(1+\sqrt{-p})\sum_{i\in Q_p} x^{ip^{\lambda-1}}+(1-\sqrt{-p})\sum_{i\in Q_p} x^{aip^{\lambda-1}}],$$

$$\theta_{-1}(x)=\frac{1-x^{p^\lambda}}{4p}[(p-1)+(1-\sqrt{-p})\sum_{i\in Q_p} x^{ip^{\lambda-1}}+(1+\sqrt{-p})\sum_{i\in Q_p} x^{aip^{\lambda-1}}],$$

where all coefficients are to be taken in $GF(q)$*, and* $\sqrt{p}$ *and* $\sqrt{-p}$ *have to be selected appropriately from the two possible values in* $GF(q)$*.*

Proof

The proof is similar to the proof of the case for $\lambda=1$.

If $p=1 \mod 4$, then $-1\in Q_{2p^\lambda}$ (cf. Lemma 2), so $a\neq -1$. Applying the relations of [4, Theorem 28 (i)] to row 0 and column 2 and to row 1 and columns 1 and a yields

$$r_\lambda - r_1\gamma - r_1\delta = 0, \tag{76}$$

$$r_\lambda + p^{1-\lambda}\gamma^2 + p^{1-\lambda}\delta^2 = p^\lambda, \tag{77}$$

$$r_\lambda + 2p^{1-\lambda}\gamma\delta = 0. \tag{78}$$

Adding and subtracting (77) and (78) and using $r_\lambda = p^{\lambda-1}(p-1)/2$ gives

$$(\gamma+\delta)^2 = p^{2\lambda-2}, \tag{79}$$

$$(\gamma-\delta)^2 = p^{2\lambda-1}, \tag{80}$$

and finally, similar to (53),

$$\gamma = \frac{1+\sqrt{p}}{2}\, p^{\lambda-1}, \quad \delta = \frac{1-\sqrt{p}}{2}\, p^{\lambda-1}. \tag{81}$$

So, we may conclude from the matrix *M* in (75) that in this case the primitive idempotent generators which correspond to columns 1 and *a* of *M* are given by (cf. also the proof of Theorem 6 (i))

$$\begin{aligned}\theta_1(x) &= (2p^\lambda)^{-1}(r_\lambda(1-x^{p^\lambda}) + \gamma\sum_{i\in C_1}(x^i - x^{i+p^\lambda}) + \delta\sum_{i\in C_a}(x^i - x^{i+p^\lambda}) \\ &= (2p^\lambda)^{-1}(1-x^{p^\lambda})(r_\lambda + \gamma\sum_{i\in Q_{p^\lambda}} x^i + \delta\sum_{i\in N_{p^\lambda}} x^i),\end{aligned}$$

with γ and δ from (81). Now, again like in the proof of Theorem 6 (i), we make use of $\sum_{i\in Q_{p^\lambda}} x^i = \sum_{i\in Q_p} x^{ip^{\lambda-1}}$ and $\sum_{i\in N_{p^\lambda}} x^i = \sum_{i\in Q_p} x^{aip^{\lambda-1}}$.

Finally, after having substituted $r_\lambda = \varphi(p^\lambda)/2 = p^{\lambda-1}(p-1)/2$, we obtain the first two expressions in the Theorem.

If $p = -1 \bmod 4$, $-1 \notin Q_{2p^\lambda}$, and so $a = -1$. We obtain from the relations [4, Theorem 28 (i)] that

$$r_\lambda - r_1\gamma - r_1\delta = 0, \tag{76}$$

$$r_\lambda + p^{1-\lambda}\gamma^2 + p^{1-\lambda}\delta^2 = 0, \tag{82}$$

$$r_\lambda + 2p^{1-\lambda}\gamma\delta = p^\lambda, \tag{83}$$

which yield in the same way as in the previous case

$$\gamma = \frac{1+\sqrt{-p}}{2}\, p^{\lambda-1}, \quad \delta = \frac{1-\sqrt{-p}}{2}\, p^{\lambda-1}. \tag{84}$$

The remaining part of the proof is completely similar to the arguments presented in the case $p = 1 \bmod 4$.

Corrolary 18

The idempotent generators of the generalized residue codes $C^i_{2p^\lambda,q,2}$, q an odd prime power with $(p,q) = 1$, $i \in \{1,a\}$, are given by $\vartheta_i(x) = 1 - \theta_i(x)$, with the polynomials $\theta_i(x)$ as defined in Theorem 17.

Example 19

Take $n = 2p^{\lambda} = 18$. So, $p = 3$ and $\lambda = 2$. We have $U_{18} = \{1,5,7,11,13,17\}$ and $Q_{18} = \{1,7,13\}$. Since 7 generates Q_{18}, we take $q = 7$. The cyclotomic cosets mod 18 with respect to 7 are $C_0 = \{0\}$, $C_1 = \{1,7,13\}$, $C_5 = \{5,17,11\}$, $C_2 = \{2,14,8\}$, $C_{10} = \{10,16,4\}$, $C_3 = \{3\}$, $C_6 = \{6\}$, $C_{12} = \{12\}$, $C_{15} = \{15\}$ and $C_9 = \{9\}$. As a consequence, we can put $a = 5(\neq -1)$.

From Theorem 17 we conclude that the idempotent generators corresponding to the columns indexed by 1 and 5 are

$$\theta_1(x) = \frac{1-x^9}{12}[2 + (1+\sqrt{-3})x^3 + (1-\sqrt{-3})x^{15}]$$

and

$$\theta_5(x) = \frac{1-x^9}{12}[2 + (1-\sqrt{-3})x^3 + (1+\sqrt{-3})x^{15}].$$

Since in $GF(7)$ we have $\sqrt{-3} = 2$ and $12^{-1} = 5^{-1} = 3$, we obtain

$$\theta_1(x) = -1 + 2x^3 - 3x^6 + x^9 - 2x^{12} + 3x^{15}$$

and

$$\theta_5(x) = -1 - 3x^3 - 2x^6 + x^9 + 3x^{12} + 2x^{15}.$$

These results correspond with the idempotents $\theta_5(x)$ and $\theta_1(x)$, respectively, as obtained in [4, Example 52]. Remember that our method does not deliver the precise correspondence between the idempotent generators and the irreducible polynomials which generate the same cyclic code.

References

1. S.K. Arora and Manju Pruthi, *Minimal Cyclic Codes of Length* $2p^n$, Finite Fields and their Applications **5** (1999), 177 – 187.
2. S. Batra and S.K. Arora, *Some Cyclic Codes of Length* $2p^n$, to be published in Designs, Codes and Cryptography, (2010).
3. S.M. Dodunekov, A. Bojilov and A.J. van Zanten, *Generalized Residue Codes,* TR 2010 – 001, TiCC, Tilburg University, www.uvt.nl/ticc
4. S.M. Dodunekov, A. Bojilov and A.J. van Zanten, *Generalized Residue Codes and their Idempotent Generators,* TR 2011, TiCC, Tilburg University, www.uvt.nl/ticc
5. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,* Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1980.
6. R.L. Lidl and Niederreiter, *Introduction to Finite Fields and their Applications* (rev. ed.), Cambridge University Press, Cambridge, 1997.

7. J.H. van Lint, *Coding Theory,* Springer-Verlag, New York, 1971.
8. J.H. van Lint and F.J. MacWilliams, *Generalized Quadratic Residue Codes,* IEEE Trans. Inf. Theory **24** (1978), 730 – 737.
9. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North Holland Publ. Company, Amsterdam, 1977.
10. V. Pless, *Introduction to the Theory of Error-Correcting Codes* (2^{nd} ed.), Wiley Intersc. Publ., John Wiley and Sons, New York, 1990.